What is claimed is:

1. A security association processor circuit, comprising:

a security association database for storing security related data for a plurality of security associations, each entry comprising security association related data corresponding to a unique socket;

means for opening a new security association upon receipt of a socket not found in said security association database;

means for searching for and recognizing a security association associated with a packet in accordance with its socket;

means for retrieving from said security association database a plurality of security related parameters; and

means for forwarding said plurality of security related parameters to a Virtual Private Networking (VPN) security processor for performing one or more security processes therewith.

2. The circuit according to claim 1, further comprising means for updating the contents of said security association database in accordance with results of said security processes.

3. The circuit according to claim 1, wherein parameters associated with said security association are configured by an entity external to said circuit and wherein said circuit comprises means for storing in said security association database security related data corresponding to said new security association in said security association database and a hash value calculated on the socket associated with said new security association.

4. The circuit according to claim 1, wherein said security association is opened by an entity external to said circuit and wherein said circuit comprises means for inserting a pointer to said new security association in a Least Recently Used (LRU) linked list.

5. The circuit according to claim 1, further comprising means for removing unused security associations from said security association database.

6. The circuit according to claim 1, further comprising means for removing unused security associations from said security association database upon exceeding a maximum timeout.

7. The circuit according to claim 1, further comprising means for removing unused security associations from said security association database upon exceeding a maximum byte count.

8. The circuit according to claim 1, wherein said means for searching for and recognizing a security association comprises:

means for calculating a hash value on the socket associated with the security association to be recognized;

means for looking up a hash pointer in a hash table using hash result as an index;

means for retrieving data from said security association database in accordance with said hash pointer; and

means for recognizing said security association if the retrieved data matches the socket associated with the packet.

9. The circuit according to claim 1, wherein said VPN security processor comprises means for performing encryption.

10. The circuit according to claim 1, wherein said VPN security processor comprises means for performing decryption.

11. The circuit according to claim 1, wherein said VPN security processor comprises means for performing authentication.

12. The circuit according to claim 1, wherein said VPN security processor comprises means for performing an IPSec specified service.

13. The circuit according to claim 1, further comprising means for applying an anti-replay mechanism to inbound packets.

14. The circuit according to claim 1, further comprising means for tracking sequence number of inbound packets.

15. The circuit according to claim 1, further comprising means for establishing and maintaining a least recently used (LRU) doubly linked list having a head and tail wherein most recently used security associations are stored at the tail and least recently used security associations are stored at the head.

16. The circuit according to claim 15, wherein in the event said LRU list is full, the security associations at the head is deleted and a new security association is added to the tail.

17. The circuit according to claim 1, wherein said socket comprises a Security Parameter Index (SPI), remote IP and Protocol components.

18. The circuit according to claim 1, wherein said security association related data comprises any one or combination of the following values: IPSec mode, encryption algorithm, encryption key.

19. The circuit according to claim 1, wherein said security association related data comprises any one or combination of the following values: IPSec mode, authentication algorithm, authentication key.

20. The circuit according to claim 1, further comprising means for rejecting said packet if an error is received from said VPN security processor.

21. The circuit according to claim 1, wherein said circuit is implemented in an Application Specific Integrated Circuit (ASIC).

22. The circuit according to claim 1, wherein said circuit is implemented in a Field Programmable Gate Array (FPGA).

23. The circuit according to claim 1, wherein said circuit is implemented in a Digital Signal Processor (DSP).

24. A Virtual Private Network (VPN) circuit, comprising:

security association database means for storing security related data for a plurality of security associations, each entry comprising security association related data corresponding to a unique socket;

a plurality of security engines, each security engine adapted to perform a security process;

means for opening a new security association upon receipt of a socket not found in said security association database means;

means for searching for and recognizing a security association associated with an input packet in accordance with its socket;

means for retrieving from said security association database means a plurality of security related parameters;

means for forwarding said plurality of security related parameters to at least one of said security engines for performing a security process therewith; and

packet building means adapted to construct an output packet in accordance with a particular security mode utilizing said input packet and the results of said security process.

25. The circuit according to claim 24, wherein at least one of said security engines is adapted to implement IPSec tunnel mode services.

26. The circuit according to claim 24, wherein at least one of said security engines is adapted to implement IPSec transport mode services.

27. The circuit according to claim 24, wherein at least one said security engine is adapted to perform encryption.

28. The circuit according to claim 24, wherein at least one said security engine is adapted to perform decryption.

28. The circuit according to claim 24, wherein at least one said security engine is adapted to perform authentication.

29. The circuit according to claim 24, wherein at least one said security engine is adapted to perform one or more IPSec services.

30. The circuit according to claim 24, wherein said circuit is implemented in an Application Specific Integrated Circuit (ASIC).

31. The circuit according to claim 24, wherein said circuit is implemented in a Field Programmable Gate Array (FPGA).

32. The circuit according to claim 24, wherein said circuit is implemented in a Digital Signal Processor (DSP).

33. A portable computing device, comprising:

communication means adapted to connect said device to a communications network;

memory means comprising volatile and non-volatile memory, said non-volatile memory adapted to store program code;

a processor coupled to said memory means and said communication means for executing said program code; and

a Virtual Private Network (VPN) circuit, comprising:

security association database means for storing security related data for a plurality of security associations, each entry comprising security association related data corresponding to a unique socket;

a plurality of security engines, each security engine adapted to perform a security process;

means for opening a new security association upon receipt of a socket not found in said security association database means;

means for searching for and recognizing a security association associated with an input packet in accordance with its socket;

means for retrieving from said security association database means a plurality of security related parameters;

means for forwarding said plurality of security related parameters to at least one of said security engines for performing a security process therewith;

packet building means adapted to construct an output packet in accordance with a particular security mode utilizing said input packet and the results of said security process.

34. The device according to claim 33, wherein said communications network comprises a Wide Area Network (WAN).

35. The device according to claim 33, wherein said communications network comprises a Local Area Network (LAN).

36. The device according to claim 33, wherein said communications network comprises the Internet.

37. The device according to claim 33, wherein said communications network comprises a Public Switched Telephone Network (PSTN).

38. The circuit according to claim 33, wherein at least one of said security engines is adapted to perform encryption.

39. The circuit according to claim 33, wherein at least one of said security engines is adapted to perform decryption.

40. The circuit according to claim 33, wherein at least one of said security engines is adapted to perform authentication.

41. The circuit according to claim 33, wherein at least one of said security engines is adapted to perform an IPSec service.

42. The circuit according to claim 33, wherein said VPN circuit is implemented in an Application Specific Integrated Circuit (ASIC).

43. The circuit according to claim 33, wherein said VPN circuit is implemented in a Field Programmable Gate Array (FPGA).

44. The circuit according to claim 33, wherein said VPN circuit is implemented in a Digital Signal Processor (DSP).

45. A security association processor circuit, comprising:

a security association database for storing security related data for a plurality of security associations, each entry comprising security association related data corresponding to a unique socket;

a management unit adapted to open a new security association upon receipt of a socket not found in said security association database;

a recognition unit adapted to search for and recognize a security association associated with an input packet in accordance with its socket;

a main processor unit adapted to retrieve from said security association database a plurality of security related parameters and forward them to a Virtual Private Networking (VPN) security processor for performing one or more security processes therewith; and

a hash unit comprising a hash function and associated hash table for facilitating the search for stored security associations.

46. The circuit according to claim 45, further comprising a least recently used (LRU) linked list adapted to provide a listing of the frequency of use of said security associations stored in said security association database.

47. The circuit according to claim 45, further comprising a packet builder adapted to construct an output packet in accordance with a particular security mode utilizing said input packet and the results of said one or more security processes.

48. The circuit according to claim 45, wherein said VPN security processor comprises means for performing encryption.

49. The circuit according to claim 45, wherein said VPN security processor comprises means for performing decryption.

50. The circuit according to claim 45, wherein said VPN security processor comprises means for performing authentication.

51. The circuit according to claim 45, wherein said VPN security processor comprises means for performing an IPSec service.

52. The circuit according to claim 45, wherein said circuit is implemented in an Application Specific Integrated Circuit (ASIC).

53. The method according to claim 45, wherein said circuit is implemented in a Field Programmable Gate Array (FPGA).

54. The method according to claim 45, wherein said circuit is implemented in a Digital Signal Processor (DSP).

55. A method of security association, said method comprising the steps of:

establishing a security association database adapted to store security related data for a plurality of security associations, each entry within said security association database corresponding to a socket;

opening a new security association upon receipt of a socket not found in said security association database;

searching for and recognizing a security association associated with a packet in accordance with its socket;

retrieving from said security association database a plurality of security related parameters; and

forwarding said plurality of security related parameters to a Virtual Private Networking (VPN) security processor for performing one or more security processes therewith.

56. The method according to claim 55, further comprising the step of updating the contents of said security association database in accordance with results of said security processes.

57. The method according to claim 55, wherein said step of opening a new security association comprises:

storing security related data corresponding to said new security association in said security association database;

calculating a hash value on the socket associated with said new security association; and

storing said hash value in a hash table.

58. The method according to claim 55, wherein said step of opening a new security association comprises inserting a pointer to said new security association in a Least Recently Used (LRU) linked list.

59. The method according to claim 55, further comprising the step of removing unused security associations from said security association database.

60. The method according to claim 55, further comprising the step of removing unused security associations from said security association database upon exceeding a maximum timeout.

61. The method according to claim 55, further comprising the step of removing unused security associations from said security association database upon exceeding a maximum byte count.

62. The method according to claim 55, wherein said step of searching for and recognizing a security association comprises the steps of:

calculating a hash value on the socket associated with the security association to be recognized;

looking up a hash pointer in a hash table using hash result as an index;

retrieving data from said security association database in accordance with said hash pointer; and

recognizing said security association if the retrieved data matches the socket associated with the packet.

63. The method according to claim 55, wherein said VPN security processor is adapted to perform encryption.

64. The method according to claim 55, wherein said VPN security processor is adapted to perform decryption.

65. The method according to claim 55, wherein said VPN security processor is adapted to perform authentication.

66. The method according to claim 55, wherein said VPN security processor is adapted to perform an IPSec specified service.

67. The method according to claim 55, further comprising the step of applying an anti-replay mechanism to packets received from a remote network.

68. The method according to claim 55, further comprising the step of tracking sequence numbers of packets received from a remote network.

69. The method according to claim 55, further comprising the step of establishing and maintaining a least recently used (LRU) doubly linked list having a head and tail wherein most recently used security associations are stored at the tail and least recently used security associations are stored at the head.

70. The method according to claim 69, wherein in the event said LRU list is full, the security associations at the head is deleted and a new security association is added to the tail.

71. The method according to claim 55, wherein said socket comprises a Security Parameter Index (SPI), remote IP and Protocol components.

72. The method according to claim 55, wherein said security association related data comprises any one or combination of the following values: IPSec mode, encryption algorithm, encryption key.

73. The method according to claim 55, wherein said security association related data comprises any one or combination of the following values: IPSec mode, authentication algorithm, authentication key.

74. The method according to claim 55, further comprising the step of rejecting said packet if an error is received from said VPN security processor.

75. The method according to claim 55, wherein said method is implemented in an Application Specific Integrated Circuit (ASIC).

76. The method according to claim 55, wherein said method is implemented in a Field Programmable Gate Array (FPGA).

77. The method according to claim 55, wherein said method is implemented in a Digital Signal Processor (DSP).

78. A computer readable storage medium having computer readable program code means embodied therein for causing a suitably programmed computer to a security association mechanism when such program is executed on said computer, said computer readable storage medium comprising:

computer readable program code means for causing said computer to establish a security association database for storing security related data for a plurality of security associations, each entry comprising security association related data corresponding to a unique socket;

computer readable program code means for causing said computer to open a new security association upon receipt of a socket not found in said security association database;

computer readable program code means for causing said computer to search for and recognizing a security association associated with a packet in accordance with its socket;

computer readable program code means for causing said computer to retrieve from said security association database a plurality of security related parameters; and

computer readable program code means for causing said computer to forward said plurality of security related parameters to a Virtual Private Networking (VPN) security processor for performing one or more security processes therewith.